SAFE DEVICES, APPS & BROWSING · MODULE 2 · CHAPTER 1

Spotting Unsafe Websites, Apps & Messages

Warning signs · Fake pop-ups · Suspicious apps · Phishing messages

⏱ 30–45 min

GRADE 6–8

🔑 Key Words

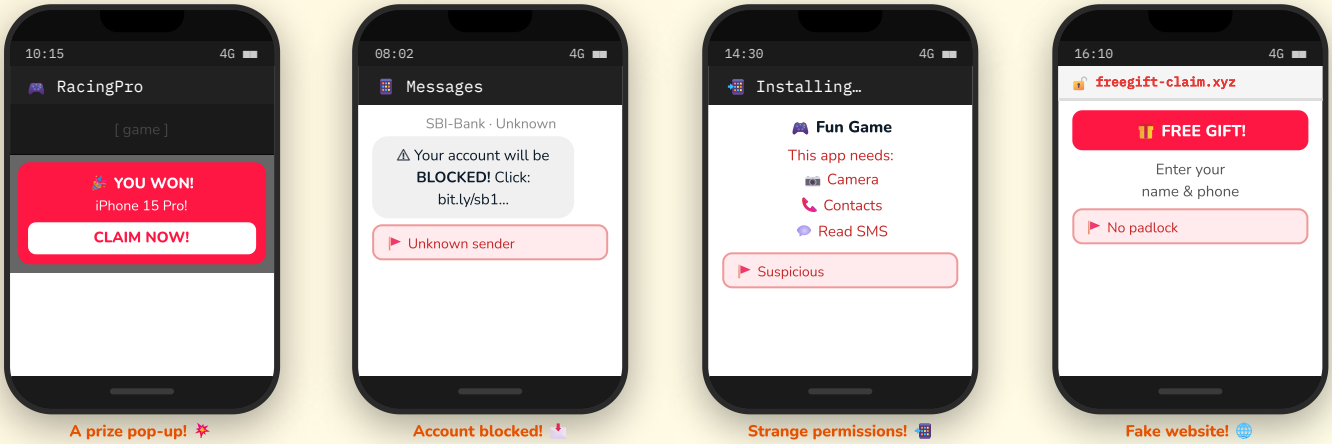
Pop-up
A box that suddenly appears. Often says "You won!" or "Virus found!" — almost always fake.

Unsafe Website
A website that tries to steal your details. Often has no 🔒 padlock in the URL.

Phishing Message
A fake message pretending to be a bank or school. It wants your OTP or password.

Warning Sign
A clue something is not safe. Like asking for your password or showing a countdown timer.

👋 Has THIS ever happened to YOU?



A prize pop-up! 💥 | Account blocked! 📩 | Strange permissions! 📲 | Fake website! 🌐

🤔 Have a think before we begin...

Q1a. Have you or someone you know seen any of these 4 things on a phone? Write YES or NO, and name one:

Q1b. What did you or that person do when it appeared? Did you click it or ignore it?

Quick Match

Q2. Match each warning sign on the LEFT to what it means on the RIGHT — draw a line

💥 A pop-up says "You won ₹1 lakh!"	(A) The website is not secure — don't enter details
🔓 Website URL shows 🔓 no padlock	(B) This is a fake prize — real companies never do this
📩 Message asks for your OTP or password	(C) The app is asking for more than it needs — suspicious
🎮 A game app asks for your contacts & SMS	(D) This is a phishing message — real banks never ask this

👥 Meet the Characters

Monica
Curious & brave. Gets tricked sometimes — but learns fast!

Rohit
Monica's older brother. Knows online safety. Explains clearly.

Sana
Monica's best friend. Careful & thoughtful. Asks good questions.

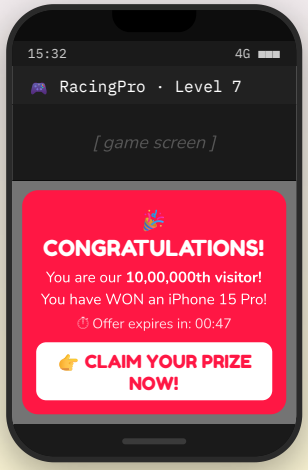
Pause & Think!

You are about to follow Monica, Rohit, and Sana as they discover dangerous things online — pop-ups, fake websites, tricky messages, and suspicious apps. **Every time they spot a warning sign — you will too.** By the end of this chapter, you will know exactly what to look for and what to do. Let's begin!

Story — Scene 1: Rohit Gets a Strange Pop-up

Scene 1 — Monica's House · Saturday Afternoon · Rohit is Gaming

Rohit: I was playing a game when suddenly — this huge pop-up appeared on my screen! Look at this, Monica!



Rohit's phone screen

Monica: Woah — you WON an iPhone?! Click CLAIM NOW! Hurry before the timer runs out!

Rohit: Monica — **STOP!** This is a FAKE pop-up. I did NOT win anything. Look at these warning signs — let me show you how to spot them.

Activity 1

Spot the Warning Signs!

Look at the pop-up above. Can you find the warning signs that Rohit spotted?

Q2. Tick ALL the warning signs in that pop-up

- ☐ It promised a prize for just visiting
- ☐ It used a countdown timer to rush you ⏱
- ☐ It was on a gaming website he trusts
- ☐ It appeared out of nowhere mid-game
- ☐ It had a big "CLAIM NOW" button
- ☐ It came from a company he had contacted

Q3. MCQ — circle one

Monica wanted Rohit to click "CLAIM NOW" quickly because of the timer. Why do fake pop-ups use countdown timers?

- ○ (A) Because the offer is really ending soon
- ○ (B) To make you panic and click without thinking
- ○ (C) To help you save time
- ○ (D) It is a normal website feature

Q3b.

Rohit did NOT click the pop-up. Monica was about to. What is the difference in how they both reacted — and why do you think Rohit knew it was fake?

Pause & Think!

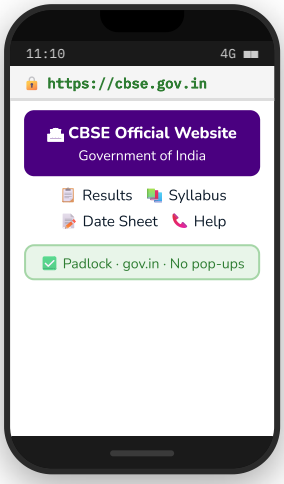
Real companies do **NOT** give away iPhones through random pop-ups. Fake pop-ups are designed to look exciting and urgent. The most important rule: **always close a pop-up — never click CLAIM or FIX.** Closing a pop-up cannot harm you. Clicking it can.

Story – Scene 2: Rohit Shows Monica Two Websites

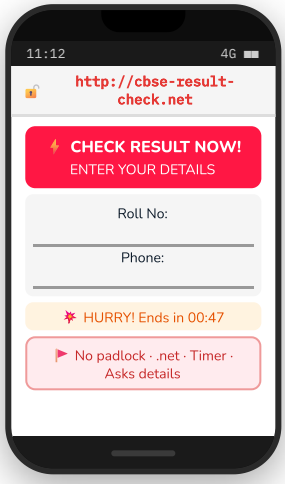
Scene 2 – Later that day · Rohit wants to check his CBSE results

Monica, I searched for my results and found TWO websites. One is real. One is fake. Can you tell me — which one is fake and which one is real?

Rohit



Website A ✅



Website B ❌

Activity 1

Real vs Fake – Help Rohit Decide!

Q4.

Fill in the table. Write what you see in each website:

Feature	Website A ✅	Website B ❌
🔒 Padlock in URL?	Yes ✅	No ❌
🌐 URL ends in .gov.in or .net?		
💥 Countdown timer?		
📋 Asks for personal details?		

Q5.

Rohit says: *"If Sana had typed her roll number and phone number into Website B — what could happen?"* Write one thing:

Pause & Think!

Rohit's rule is simple: a real website always has a 🔒 **padlock** in the URL bar and ends in **.gov.in / .edu / .org / .com**. Fake websites rush you with countdown timers and ask for personal details suddenly. **Slow down. Check the URL. Never enter your details on a website you don't trust.**

How to Check if a Website is Real – Rohit's Quick Rules

- 🔒 Look for the **padlock** in the URL bar
- 🌐 URL should end in **.gov.in / .edu / .org**
- ⚡ Ignore **countdown timers** — they are tricks
- 🚫 Real sites don't suddenly ask for your **phone or address**

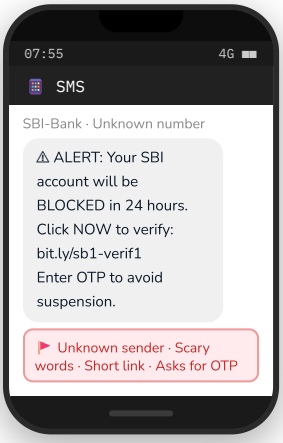
Story — Scene 3: Monica Gets a Scary Message

Scene 3 — The Next Morning · Monica's Phone Buzzes

Monica: Rohit! I got this SMS and I am scared. It says my SBI account will be BLOCKED! I don't even have an SBI account!

Rohit: That is called **PHISHING**, Monica. The message is fake — it WANTS you to feel scared so you click the link fast without thinking. Show me.

Sana: Wait — you said you don't even have an SBI account! So how can it be your account that is "blocked"? That's already a clue it's fake!



Rohit points out the clues — can you see them?

- ⚠ **Clue 1:** "BLOCKED in 24 hours" — scary words to make you panic
- ⚠ **Clue 2:** Short link "bit.ly/sb1-verif1" — hides the real destination
- ⚠ **Clue 3:** Asks for your OTP — real banks NEVER ask for OTP over SMS
- ⚠ **Clue 4:** Monica doesn't even have an SBI account — sent to random numbers

Activity 2

Analyse Monica's Fake Message

Q6. Tick ✓ ALL the warning signs in the SMS

- ☐ It came from an unknown number — not the real SBI bank number
- ☐ It used urgent words like "BLOCKED" and "24 hours"
- ☐ It had a short, strange link (bit.ly) that hides where it really goes
- ☐ It asked Monica to enter her OTP — which real banks never ask
- ☐ It was written in clear, polite English with no urgency

Q6a. Spot the Difference — look at these two messages. Circle every difference you can find

Message A — Fake

WhatsApp · Unknown Number +91 99XXX

Congrats! You have won a FREE ₹500 Jio recharge! You are our LUCKY winner today! Claim NOW before it expires: bit.ly/free-jiowinner — Hurry! Offer ends in 10 mins! ⏱

Message B — Real

WhatsApp · Jio Official ✓ Verified

Dear Customer, your Jio plan is active till 14 April 2026. To recharge, open the MyJio app or visit jio.com. For help call 199.

I found _____ differences. The BIGGEST warning sign in Message A is:

Q6b.

Rohit says: *"This fake Jio message was sent to thousands of people — most of them will never even use Jio."* Why do scammers send the same fake message to so many random people?

Q7.

Sana said: *"This message came even though Rohit does not use Jio!"* What does this tell you about phishing messages?

Pause & Think!

Phishing messages are sent to **thousands of random numbers** at once. They don't know who you are. They just hope someone panics and clicks. **Real banks never ask for your OTP or password over SMS or WhatsApp.** If you receive a scary message — don't click, don't reply. Show it to a trusted adult.

Story – Scene 4: Sana Wants to Download a New App

Scene 4 – Evening · Sana Shows Rohit an App She Found

Sana: Rohit bhai, I want to download this racing game. But it is asking for so many things before installing. Is that normal?

Rohit: Let me see. **looks at screen** Sana — this racing game is asking for your **Camera, Contacts, Phone Calls, and SMS**. That is NOT normal for a game. Do NOT install this!

Monica: I get it now! A racing game only needs to show on screen and play sounds. It has NO reason to read my contacts or phone calls. That is a warning sign!

Activity 3

Does This Permission Make Sense?

Rohit's rule: **"An app should only ask for what it needs to work."** Sort each permission below.

1. Location — Weather App
2. Camera — Racing Game
3. Notifications — Weather App
4. Phone Calls — Racing Game
5. Read SMS — Racing Game
6. Payments — Weather App
7. Play Audio — Racing Game
8. Camera — Video Call App

Makes Sense (App needs this)

Write numbers here...

Suspicious (App does NOT need this)

Write numbers here...

Q8.

Sana's racing game was asking for Camera + Contacts + Phone Calls + SMS. Monica says "don't install it." Do you agree? Write YES or NO and one reason:

Draw & Match

Q9. Match each app to the ONE permission it actually needs — draw a line

Camera App — Takes photos	(A) Location — to show weather near you
Weather App — Shows forecast	(B) Camera — to take photos
Video Call App — Calls friends	(C) Camera + Microphone — to video call
Torch App — Turns on light	(D) Flashlight only — nothing else

Bonus: If a Torch App asked for your Contacts and Location — would you install it? Write YES or NO and why:

Pause & Think!

Before installing ANY app — ask yourself: **"Does this app actually need this permission to do its job?"** A torch doesn't need your contacts. A game doesn't need your phone calls. **Extra permissions = warning sign. Don't install it.**

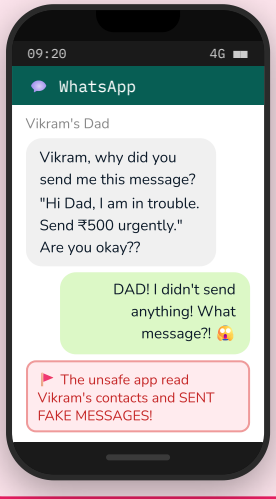
Story – Scene 5: What Happened to Vikram?

Scene 5 – The Next Day at School · Monica tells the story of her cousin Vikram

Monica

> You know my cousin Vikram? He downloaded a game called SpeedBlast Pro from a random website — NOT the Play Store. Two days later something scary happened...

What Happened to Vikram – Case Study



What Vikram did:

- Downloaded SpeedBlast from **a random website**
- ⚠ App asked for Contacts + SMS — he clicked **Allow**
- **Malware hid inside the app** — read all his contacts
- **Sent fake messages** pretending to be Vikram asking for money

Activity 4

Analyse Vikram's Case

Q9. Tick ALL the mistakes Vikram made

- [ ] He downloaded the app from a random website, not the Play Store
- [ ] He allowed Contacts and SMS permissions for a racing game
- [ ] He played a racing game on his phone
- [ ] He did not check what permissions the app was asking for

Q10.

Monica says: ***"Vikram thought it was safe because his friend told him about it."*** Why is this NOT a good reason to trust a download?

Q11. Two sides – circle ONE and write why

Vikram says:
"I didn't know the app was unsafe. It wasn't my fault."

Rohit says:
"You should always check permissions and only use the official Play Store — before clicking Allow."

I agree with _____ because:

Pause & Think!

Vikram's friend probably didn't know the app was dangerous either — they just shared it. This is how unsafe apps spread. **Even trusted people can accidentally share unsafe links.** The rule is always: **check the source, check the permissions, use only the official store.**

Story — Scene 6: The Group Puts It All Together

1

OK — so pop-ups, fake sites, scary SMS, dodgy apps. I now know what to look for!

Monica is determined!

2

Three rules. Stop. Think. Check. Before you click ANYTHING suspicious!

Rohit summarises!

3

And always tell a trusted adult when something feels wrong!

Sana adds!

4

Together: STOP · THINK · CHECK · TELL! We are Cyber Safety Champions!

All three together!

Activity 5 — Is It Safe?

Quick Check — 4 Situations

The group made this quick check for Vikram. Tick ✓ **SAFE** or **NOT SAFE** and write one reason.

Situation A

Sana visits **https://ncert.nic.in** to download her textbook. The URL has a padlock.

☐ SAFE ☐ NOT SAFE

Reason:

Situation B

A pop-up says: *"⚠ VIRUS on your phone! Download our FREE cleaner app NOW!"*

☐ SAFE ☐ NOT SAFE

Reason:

Situation C

Rohit installs a calculator app from Google Play Store. It only asks for **storage** to save history.

☐ SAFE ☐ NOT SAFE

Reason:

Situation D

Monica gets a message: *"You won a FREE trip to Goa! Enter your Aadhaar number to claim."*

☐ SAFE ☐ NOT SAFE

Reason:

Q12. Odd One Out — circle the SAFE one, explain why the others are not

"You won ₹1 lakh!" (pop-up)	https:// ncert.nic.in (website)	"Free iPhone share bank details" (message)	Game needs camera + contacts (app)

The SAFE one is: _____ Because:

Pause & Think!

You now know three types of online traps: **fake websites** (no padlock, strange URL), **suspicious apps** (too many unnecessary permissions), and **fake messages** (unknown sender, urgent tone, asks for OTP or money). Spot the sign. Stop and think. **Tell a trusted adult.**

Pause & Think!

You followed Monica, Rohit, and Sana through 6 scenes. You spotted fake pop-ups, fake websites, phishing messages, and suspicious app permissions. **You are now a Cyber Safety spotter!** In Chapter 2 — Sana makes a mistake. Will you be able to spot it before she does?

Quick Revision – Test Yourself!

Quick Revision

Q13. MCQ – circle one

You see a pop-up: "CONGRATULATIONS! You won an iPhone!" What do you do?

- ○ (A) Click CLAIM NOW quickly
- ○ (B) Close it. It is fake.
- ○ (C) Share your address to claim
- ○ (D) Ask your friend to click it

Q14. MCQ – circle one

A website has 🔓 (no padlock) in the URL. This means:

- ○ (A) The website is new
- ○ (B) Not secure — do NOT enter details
- ○ (C) The padlock is broken — tell the site
- ○ (D) It only works on WiFi

Q15. Match – draw a line to the right column

Pop-up promising a free prize	→ ⚠ Warning Sign
🔓 Website with no padlock	→ ⚠ Warning Sign
🎮 Game asking for your contacts	→ ⚠ Warning Sign
🔒 URL starts with https://	→ ✅ Safe Sign
📲 App from official Play Store	→ ✅ Safe Sign

Key Takeaways

Fake Pop-ups Are Tricks
"You won a prize!" is almost always fake. Close it. Never click CLAIM or FIX.

Check the URL Padlock
A real website has 🔒 in the URL. No padlock = not secure. Don't enter details.

Fake Messages Use Fear
Scary words + unknown number + strange links = phishing. Don't click. Tell an adult.

Check App Permissions
Ask: does this app need this? If not — warning sign. Don't install it.

🏆 Monica, Rohit & Sana's Golden Rule

*"Before you click ANYTHING suspicious — **STOP. THINK. CHECK.***
🔒 Padlock in URL? · 📲 Permissions make sense? · 💌 Sender known to me?
*Not sure? **Close it. Tell a trusted adult. Stay safe.** 🛡"*